CLAIMS

1. An apparatus in a microprocessor, for accomplishing cryptographic operations, comprising:

translation logic, configured to receive a cryptographic instruction from a source therefrom, wherein said cryptographic instruction prescribes one of the cryptographic operations, and configured to translate said cryptographic instruction into a sequence of micro instructions specifying sub-operations required to accomplish said one of the cryptographic operations; and

execution logic, operatively coupled to said translation logic, configured to receive said sequence of micro instructions, and configured to perform said sub-operations.

2. The apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished at the level of system privileges afforded to application programs.

3. The apparatus as recited in claim 1, wherein said one of the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

4. The apparatus as recited in claim 1, wherein said one of the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

5. The apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

6. The apparatus as recited in claim 1, wherein said cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations.

7. The apparatus as recited in claim 6, wherein said block cipher mode comprises electronic code book (ECB) mode.

8. The apparatus as recited in claim 6, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

9. The apparatus as recited in claim 6, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

10. The apparatus as recited in claim 6, wherein said block cipher mode comprises output feedback (OFB) mode.

11. The apparatus as recited in claim 1, wherein said cryptographic instruction prescribes that said one of the cryptographic operations be accomplished on a plurality of text blocks.

12. The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

13. The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within the microprocessor.

14. The apparatus as recited in claim 13, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

15. The apparatus as recited in claim 13, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

16. The apparatus as recited in claim 13, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

17. The apparatus as recited in claim 13, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

18. The apparatus as recited in claim 17, wherein said cryptographic key data comprises a cryptographic key.

19. The apparatus as recited in claim 17, wherein said cryptographic key data comprises a cryptographic key schedule.

20. The apparatus as recited in claim 13, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

21. The apparatus as recited in claim 13, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

22. The apparatus as recited in claim 21, wherein said control word comprises:

an encryption/decryption field, configured to prescribe whether said one of the cryptographic operations is an encryption operation or a decryption operation.

23. The apparatus as recited in claim 1, wherein said execution logic comprises:

a cryptography unit, configured to receive a first plurality of said sequence of micro instructions, and configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

24. The apparatus as recited in claim 23, wherein said cryptography unit comprises:

block cipher logic, configured to perform said plurality of cryptographic rounds on said each of a plurality of input text blocks according to said one of the cryptographic operations to produce said corresponding each of a plurality of output text blocks; and

key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to each of said plurality of cryptographic rounds, and configured to provide said each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds.

25. The apparatus as recited in claim 23, wherein said block cipher logic is divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more input text blocks.

26. The apparatus as recited in claim 23, wherein said execution logic further comprises:

an integer unit, coupled in parallel with said cryptography unit, configured to receive a second plurality of said sequence of micro instructions, and configured to execute a plurality of integer operations that are required to accomplish said one of the cryptographic operations.

27. The apparatus as recited in claim 23, wherein said sequence of micro instructions comprises:

a first micro instruction, configured to direct said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds.

28. A microprocessor apparatus, for performing cryptographic operations, comprising:

a cryptographic instruction, received by a microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations; and

translation logic, configured to translate said cryptographic instruction into associated micro instructions that specify sub-operations required to accomplish said one of the cryptographic operations

29. The microprocessor apparatus as recited in claim 28, wherein said one of the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

30. The microprocessor apparatus as recited in claim 28, wherein said one of the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

31. The microprocessor apparatus as recited in claim 28, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

32. The microprocessor apparatus as recited in claim 28, wherein said cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations.

33. The microprocessor apparatus as recited in claim 32, wherein said block cipher mode comprises electronic code book (ECB) mode.

34. The microprocessor apparatus as recited in claim 32, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

35. The microprocessor apparatus as recited in claim 32, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

36. The microprocessor apparatus as recited in claim 32, wherein said block cipher mode comprises output feedback (OFB) mode.

37. The microprocessor apparatus as recited in claim 28, wherein said cryptographic instruction prescribes that said one of the cryptographic operations be accomplished on a plurality of text blocks.

38. The microprocessor apparatus as recited in claim 28, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

39. The microprocessor apparatus as recited in claim 28, wherein said cryptographic instruction implicitly references a plurality of registers within said microprocessor.

40. The microprocessor apparatus as recited in claim 39, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

41. The microprocessor apparatus as recited in claim 39, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

42. The microprocessor apparatus as recited in claim 39, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

43. The microprocessor apparatus as recited in claim 39, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

44. The microprocessor apparatus as recited in claim 43, wherein said cryptographic key data comprises a cryptographic key.

45. The microprocessor apparatus as recited in claim 43, wherein said cryptographic key data comprises a cryptographic key schedule.

46. The microprocessor apparatus as recited in claim 39, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

47. The microprocessor apparatus as recited in claim 39, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

48. The microprocessor apparatus as recited in claim 47, wherein said control word comprises:

an encryption/decryption field, configured to prescribe whether said one of the cryptographic operations is an encryption operation or a decryption operation.

49. The microprocessor apparatus as recited in claim 28, further comprising:

execution logic, operatively coupled to said translation logic, configured to receive said associated micro instructions, and configured to perform said sub-operations.

50. The microprocessor apparatus as recited in claim 49, wherein said execution logic comprises:

a cryptography unit, configured to receive a first plurality of said associated micro instructions, and configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

51. The microprocessor apparatus as recited in claim 50, wherein said cryptography unit comprises:

block cipher logic, configured to perform said plurality of cryptographic rounds on said each of a plurality of input text blocks according to said one of the block cryptographic operations to produce said corresponding each of a plurality of output text blocks; and

key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to each of said plurality of cryptographic rounds, and configured to provide said each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds.

52. The microprocessor apparatus as recited in claim 51, wherein said block cipher logic is divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more input text blocks.

53. The microprocessor apparatus as recited in claim 50, wherein said execution logic further comprises:

an integer unit, coupled in parallel with said cryptography unit, configured to receive a second plurality of said associated micro instructions, and configured to execute a plurality of integer operations that are required to accomplish said one of the cryptographic operations.

54. The microprocessor apparatus as recited in claim 50, wherein said associated micro instructions comprise:

a first micro instruction, configured to direct said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds.

55. The microprocessor apparatus as recited in claim 28, wherein said application program executes on said microprocessor at the level of system privileges afforded to application programs.

56. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by logic within a processor, wherein said cryptographic instruction prescribes one of the cryptographic operations; and

execution logic, coupled to said logic, configured to perform said one of the cryptographic operations.

57. The apparatus as recited in claim 56, wherein said one of the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

58. The apparatus as recited in claim 56, wherein said one of the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

59. The apparatus as recited in claim 56, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

60. The apparatus as recited in claim 56, wherein said cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations.

61. The apparatus as recited in claim 60, wherein said block cipher mode comprises electronic code book (ECB) mode.

62. The apparatus as recited in claim 60, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

63. The apparatus as recited in claim 60, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

64. The apparatus as recited in claim 60, wherein said block cipher mode comprises output feedback (OFB) mode.

65. The apparatus as recited in claim 60, wherein said cryptographic instruction prescribes that said one of the cryptographic operations be accomplished on a plurality of text blocks.

66. The apparatus as recited in claim 60, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

67. The apparatus as recited in claim 56, wherein said cryptographic instruction implicitly references a plurality of registers within said processor.

68. The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

69. The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

70. The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

71. The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

72. The apparatus as recited in claim 71, wherein said cryptographic key data comprises a cryptographic key.

73. The apparatus as recited in claim 71, wherein said cryptographic key data comprises a cryptographic key schedule.

74. The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

75. The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

76. The apparatus as recited in claim 75, wherein said control word comprises:

an encryption/decryption field, configured to prescribe whether said one of the cryptographic operations is an encryption operation or a decryption operation.

77. The apparatus as recited in claim 56, further comprising:

translation logic, configured to translate said cryptographic instruction into associated micro instructions that specify sub-operations required to accomplish said one of the cryptographic operations.

78. The apparatus as recited in claim 77, wherein said execution logic comprises:

a cryptography unit, configured to receive a first plurality of said associated micro instructions, and configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

79. The apparatus as recited in claim 78, wherein said cryptography unit comprises:

block cipher logic, configured to perform said plurality of cryptographic rounds on said each of a plurality of input text blocks according to said one of the block cryptographic operations to produce said corresponding each of a plurality of output text blocks; and

key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to each of said plurality of cryptographic rounds, and configured to provide said each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds.

80. The apparatus as recited in claim 79, wherein said block cipher logic is divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more input text blocks.

81. The apparatus as recited in claim 78, wherein said execution logic further comprises:

an integer unit, coupled in parallel with said cryptography unit, configured to receive a second plurality of said associated micro instructions, and configured to execute a plurality of integer operations that are required to accomplish said one of the cryptographic operations.

82. The apparatus as recited in claim 78, wherein said associated micro instructions comprise:

a first micro instruction, configured to direct said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds.

83. The apparatus as recited in claim 56, wherein said one of the cryptographic operations is accomplished at the privilege level afforded to application programs.

84. A method for performing cryptographic operations in a processor, the method comprising:

receiving a cryptographic instruction, wherein the cryptographic instruction prescribes one of the cryptographic operations; and

executing the one of the cryptographic operations.

85. The method as recited in claim 84, wherein said receiving comprises:

prescribing an encryption operation as the one of the cryptographic operations, wherein the encryption operation comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

86. The method as recited in claim 84, wherein said receiving comprises:

prescribing a decryption operation as the one of the cryptographic operations, wherein the decryption operation comprises decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

87. The method as recited in claim 84, wherein said executing comprises:

accomplishing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

88. The method as recited in claim 84, wherein said receiving comprises:

specifying, within the cryptographic instruction, a block cipher mode to be employed in accomplishing the one of the cryptographic operations.

89. The method as recited in claim 88, wherein the block cipher mode comprises electronic code book (ECB) mode.

90. The method as recited in claim 88, wherein the block cipher mode comprises cipher block chaining (CBC) mode.

91. The method as recited in claim 88, wherein the block cipher mode comprises cipher feedback mode (CFB) mode.

92. The method as recited in claim 88, wherein the block cipher mode comprises output feedback (OFB) mode.

93. The method as recited in claim 84, wherein said receiving comprises:

specifying, within the cryptographic instruction, that the one of the cryptographic operations is to be accomplished on a plurality of text blocks.

94. The method as recited in claim 84, wherein said receiving comprises:

prescribing the block cryptographic instruction according to the x86 instruction format.

95. The method as recited in claim 84, wherein said receiving comprises:

implicitly referencing a plurality of registers within the processor.

96. The method as recited in claim 95, wherein said implicitly referencing comprises:

first referencing a first register, wherein contents of the first register comprise a first pointer to a first memory address, the first memory address specifying a first location in memory for access of a plurality of input text blocks upon which the one of the cryptographic operations is to be accomplished.

97. The method as recited in claim 95, wherein said implicitly referencing comprises:

second referencing a second register, wherein contents of the second register comprise a second pointer to a second memory address, the second memory address specifying a second location in the memory for storage of a corresponding plurality of output text blocks, the corresponding plurality of output text blocks being generated as a result of said executing the one of the cryptographic operations upon a plurality of input text blocks.

98. The method as recited in claim 95, wherein said implicitly referencing comprises:

third referencing a third register, wherein contents of the third register indicate a number of text blocks within a plurality of input text blocks.

99. The method as recited in claim 95, wherein said implicitly referencing comprises:

fourth referencing a fourth register, wherein contents of the fourth register comprise a third pointer to a third memory address, the third memory address specifying a third location in memory for access of cryptographic key data for use in said executing the one of the cryptographic operations.

100. The method as recited in claim 99, wherein the cryptographic key data comprises a cryptographic key.

101. The method as recited in claim 99, wherein the cryptographic key data comprises a cryptographic key schedule.

102. The method as recited in claim 95, wherein said implicitly referencing comprises:

fifth referencing a fifth register, wherein contents of the fifth register comprise a fourth pointer to a fourth memory address, the fourth memory address specifying a fourth location in memory for access of an initialization vector for use in said executing the one of the cryptographic operations.

103. The method as recited in claim 95, wherein said implicitly referencing comprises:

sixth referencing a sixth register, wherein contents of the sixth register comprise a fifth pointer to a fifth memory address, the fifth memory address specifying a fifth location in memory for access of a control word for use in said executing the one of the cryptographic operations, said fifth referencing comprising:

prescribing, within the control word, cryptographic parameters for the one of the cryptographic operation.

104. The method as recited in claim 103, wherein said prescribing comprises:

indicating, via an encryption/decryption field within the control word, whether the one of the cryptographic operations is an encryption operation or a decryption operation.

105. The method as recited in claim 84, further comprising:

translating the cryptographic instruction into a sequence of micro instructions that specify sub-operations to be performed as part of said executing.

106. The method as recited in claim 84, wherein said executing comprises:

first routing a first plurality of the sequence of micro instructions to a cryptography unit; and

within the cryptography unit, first accomplishing a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein the plurality of cryptographic rounds are prescribed by a control word that is provided to the cryptography unit.

107. The method as recited in claim 106, wherein said first accomplishing comprises:

storing a key schedule within the cryptography unit, the key schedule comprising a plurality of round keys, each corresponding to each of a plurality of cryptographic rounds; and

using each of the plurality of round keys to for performance of the each of the plurality of cryptographic rounds.

108. The method as recited in claim 106, wherein said executing further comprises:

second routing a second plurality of the sequence of micro instructions to an integer unit that is coupled in parallel with the cryptography unit; and

within the integer unit, second accomplishing a plurality of integer operations that are required for said executing the one of the cryptographic operations.

109. The method as recited in claim 105, wherein said translating comprises:

generating a first micro instruction that directs the cryptography unit to load one of the each of the plurality of input text blocks and to perform the plurality of cryptographic rounds.

110. The method as recited in claim 81, wherein said executing is accomplished at the privilege level afforded to application programs.